Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the above-identified applications:

Listing of Claims:

1-16 **(Canceled)**

17. (New) A method in a computer system for employing a digital certificate, for use only within said computer system, to authenticate operations internal to said computer system, said method comprising:

storing a master key pair and data specifying an authentication code in a protected storage within a security subsystem, wherein said master key pair comprises a first private key and a first public key and said first private key and said authentication code are inaccessible outside of said security subsystem;

receiving a request to generate a digital certificate at said security subsystem;

generating a user prompt for said authentication code in response to a receipt of said request to generate said digital certificate;

receiving a reply from a user in response to a generation of said user prompt; and

processing said request to generate said digital certificate in response to a receipt of said reply, wherein said processing comprises

generating said digital certificate utilizing said first private key only if said reply is determined to correctly specify said authentication code, wherein said digital certificate comprises data specifying a second public key of a target key pair.

18. (New) The method of claim 17, wherein said request to generate said digital certificate comprises said data specifying said second public key.

19. (New) The method of claim 17, wherein generating said digital certificate comprises:
comparing data of said reply to said authentication code; and
generating said digital certificate in response to a comparison of said data of said reply and said authentication code.

20. (New) The method of claim 17, wherein generating said digital certificate comprises:
performing a hashing operation on said data specifying said second public key to produce a hashed value;
performing an encryption operation on said hashed value utilizing said first private key to produce an digital signature; and
appending said digital signature to said second public key to produce said digital certificate.

21. (New) The method of claim 17, wherein generating said digital certificate comprises:
appending a certificate identifier to said second public key to produce security data, wherein said certificate identifier uniquely identifies said digital certificate within said computer system;
performing a hashing operation on said security data to produce a hashed value;
performing an encryption operation on said hashed value utilizing said first private key to produce an digital signature; and
appending said digital signature to said security data to produce said digital certificate.

22. (New) The method of claim 20, further comprising:
receiving a request to validate said digital certificate;
accessing said first public key within said protected storage;
performing a decryption operation on said digital signature utilizing said first public key to produce a first hashed value;
performing said hashing operation on said second public key to produce a second hashed value; and
comparing said first hashed value and said second hashed value.

23. (New) A computer system for employing a digital certificate for use only within said computer system to authenticate operations internal to said computer system, said computer system comprising:

means for storing a master key pair and data specifying an authentication code in a protected storage within a security subsystem, wherein said master key pair comprises a first private key and a first public key and said first private key and said authentication code are inaccessible outside of said security subsystem;

means for receiving a request to generate a digital certificate at said security subsystem;

means for generating a user prompt for said authentication code in response to a receipt of said request to generate said digital certificate;

means for receiving a reply from a user in response to a generation of said user prompt; and

means for processing said request to generate said digital certificate in response to a receipt of said reply, wherein said means for processing comprises

means for generating said digital certificate utilizing said first private key only if said reply is determined to correctly specify said authentication code, wherein

said digital certificate comprises data specifying a second public key of a target key pair.

24. (New) The computer system of claim 23, wherein said request to generate said digital certificate comprises said data specifying said second public key.

25. (New) The computer system of claim 23, wherein means for generating said digital certificate comprises:

means for comparing data of said reply to said authentication code; and

means for generating said digital certificate in response to a comparison of said data of said reply and said authentication code.

26. (New) The computer system of claim 23, wherein said means for generating said digital certificate comprises:

means for performing a hashing operation on said data specifying said second public key to produce a hashed value;

means for performing an encryption operation on said hashed value utilizing said first private key to produce an digital signature; and

means for appending said digital signature to said second public key to produce said digital certificate.

27. (New) The computer system of claim 23, wherein said means for generating said digital certificate comprises:

means for appending a certificate identifier to said second public key to produce security data, wherein said certificate identifier uniquely identifies said digital certificate within said computer system;

means for performing a hashing operation on said security data to produce a hashed value;

means for performing an encryption operation on said hashed value utilizing said first private key to produce an digital signature; and

means for appending said digital signature to said security data to produce said digital certificate.

28. (New) The computer system of claim 26, further comprising:

means for receiving a request to validate said digital certificate;

means for accessing said first public key within said protected storage;

means for performing a decryption operation on said digital signature utilizing said first public key to produce a first hashed value;

means for performing said hashing operation on said second public key to produce a second hashed value; and

means for comparing said first hashed value and said second hashed value.

29. (New) A computer-readable medium encoded with a computer program, which when executed by a processor, causes said processor to implement a method in a computer system for employing a digital certificate, for use only within said computer system, to authenticate operations internal to said computer system, said method comprising:

storing a master key pair and data specifying an authentication code in a protected storage within a security subsystem, wherein said master key pair comprises a first private

key and a first public key and said first private key and said authentication code are inaccessible outside of said security subsystem;

receiving a request to generate a digital certificate at said security subsystem;

generating a user prompt for said authentication code in response to a receipt of said request to generate said digital certificate;

receiving a reply from a user in response to a generation of said user prompt; and

processing said request to generate said digital certificate in response to a receipt of said reply, wherein said processing comprises

generating said digital certificate utilizing said first private key only if said reply is determined to correctly specify said authentication code, wherein said digital certificate comprises data specifying a second public key of a target key pair.

30. (New) The computer-readable medium of claim 29, wherein said request to generate said digital certificate comprises said data specifying said second public key.

31. (New) The computer-readable medium of claim 29, wherein generating said digital certificate comprises:

comparing data of said reply to said authentication code; and

generating said digital certificate in response to a comparison of said data of said reply and said authentication code.

32. (New) The computer-readable medium of claim 29, wherein generating said digital certificate comprises:

performing a hashing operation on said data specifying said second public key to produce a hashed value;

performing an encryption operation on said hashed value utilizing said first private key to produce an digital signature; and

appending said digital signature to said second public key to produce said digital certificate.

33. (New) The computer-readable medium of claim 29, wherein generating said digital certificate comprises:

appending a certificate identifier to said second public key to produce security data, wherein said certificate identifier uniquely identifies said digital certificate within said computer system;

performing a hashing operation on said security data to produce a hashed value;

performing an encryption operation on said hashed value utilizing said first private key to produce an digital signature; and

appending said digital signature to said security data to produce said digital certificate.

34. (New) The computer-readable medium of claim 32, said method further comprising:

receiving a request to validate said digital certificate;

accessing said first public key within said protected storage;

performing a decryption operation on said digital signature utilizing said first public key to produce a first hashed value;

performing said hashing operation on said second public key to produce a second hashed value; and

comparing said first hashed value and said second hashed value.